AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

United States of America
v.
Christopher VOLDEN

Case No. 2:21 mj 478

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 07/14/2021 in the county of Franklin in the Southern District of Ohio, the defendant(s) violated:

Code Section	*Offense Description*
21 USC Section 841	Possession with Intent to distribute LSD and MDMA
21 USC Section 846	Conspiracy to manufacture, distribute, possess with intent to distribute LSD and MDMA

This criminal complaint is based on these facts:

See attached affidavit, which is incorporated by reference.

☑ Continued on the attached sheet.

TFO
Complainant's signature

TFO Andrew Wuertz
Printed name and title

Sworn to before me and signed in my presence. CONSISTENT WITH FRCRP 4.1 (b)(2)(A). NMK

Date: 7/20/2021

Judge's signature

City and state: Columbus, Ohio

N. m. King,
~~Elizabeth Preston Deavers~~, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, Andrew Wuertz, being duly sworn, state:

INTRODUCTION

1. I am a Task Force Officer with the DEA and have been since May of 2010. I am assigned to the Central Ohio Cyber Drug Task Force (COCDTF) in Columbus, Ohio, where I am is responsible for conducting narcotics investigations involving dark web marketplaces. Prior to becoming a Task Force Officer, I have been employed as an Upper Arlington Police Officer for 24 years. While working with the DEA, I was assigned to the COCDTF with other law enforcement agencies targeting drug and weapon shipments purchased off the internet. As a Task Force Officer, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. Since working with the DEA, I have been involved in narcotics-related arrests, executed search warrants that resulted in the seizure of narcotics, and participated in narcotics investigations. Through training and experience, I am familiar with the manner in which persons involved in the illicit distribution of controlled substances often operate. In particular, I am aware that drug traffickers often communicate with their customers, couriers, and/or associates through the use of standard hardline telephones, and cellular telephones, or use of multiple telephones or other devices, to avoid detection by law enforcement.

2. I have participated in and conducted numerous investigations of violations of various state and federal criminal laws, including violations of Title 21 United States Code.

PURPOSE OF AFFIDAVIT

3. I am participating in an investigation concerning an organized group of known and unknown individuals who are suspected of involvement in criminal offenses against the United States, namely, to manufacture, distribute or dispense a controlled substance, in violation of 21 U.S.C. § 841 and 21 U.S.C. § 846.

4. The information set forth in this affidavit is based upon my knowledge, training, experience, and participation in investigations involving the smuggling, possession, distribution, and storage of narcotics and narcotics proceeds. This information is also based on the knowledge, training, experience, and investigations conducted by fellow law enforcement officers, who have reported to me either directly or indirectly. I believe this information to be true and reliable. I know according to the Federal Analogue Act, 21 U.S.C. § 813 any chemical substantially similar to a controlled substance listed in Schedule I or II of the Drug Enforcement Administration's (DEA) Controlled Substance Schedule is to be treated as if it were listed in Schedule I, if intended for human consumption. I know is it is a violation of 21 U.S.C. § 841 to manufacture, distribute or dispense a controlled substance and a violation of 21 U.S.C. § 846 to attempt or conspire to manufacture, distribute or dispense a controlled substance.

5. The information contained in this affidavit is based upon my personal participation in this investigation, information obtained from other agents and detectives assisting in this investigation, and my review of records, documents, and other material relating to this investigation.

6. Because this affidavit is being submitted for the limited purpose of securing criminal complaints and arrest warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to

establish probable cause to believe that Christopher VOLDEN violated 21 U.S.C. § 841 and 21 U.S.C. § 846.

BACKGROUND ON THE DARK WEB & CRYPTOCURRENCY

7. Based on my training, research, education, and experience, I am familiar with the following relevant terms and definitions:

a. The "dark web" is a portion of the "deep web[1]" of the Internet, where individuals must use an anonymizing software or application called a "darknet" to access content and websites. Within the dark web, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web" or simply the "web"). These online market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring. Famous dark web marketplaces ("DWM's"), also called Hidden Services, such as Silk Road 1, Silk Road 2, AlphaBay, and Hansa (all of which have since been shut down by law enforcement), operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services. When law enforcement shut down the four DWM's listed above, they also obtained images of their servers, and law enforcement has been able to mine the data from those sites for information about the customers and vendors who used them.

[1] The deep web is the portion of the Internet not indexed by search engines. Examples are databases and internal networks belonging to private industry, government agencies, or academic institutions.

b. "Vendors" are the dark web's sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of "vendor accounts" on dark web marketplaces. Customers, meanwhile, operate "customer accounts." Vendor and customer accounts are not identified by numbers, but rather monikers or "handles," much like the username one would use on a clear web site. If a moniker on a particular marketplace has not already been registered by another user, vendors and customers can use the same moniker across multiple marketplaces, and based on seller and customer reviews, can become well known as "trusted" vendors or customers. It is also possible for the same person to operate multiple customer accounts and multiple vendor accounts at the same time. For example, based on my training and experience, I know that one person could have a vendor account that he or she uses to sell illegal goods on a dark web marketplace in exchange for cryptocurrency; that same vendor could also have a different customer account that he or she uses to exchange cryptocurrency earned from vendor sales for fiat currency[2]. Because they are separate accounts, a person could use different accounts to send and receive the same cryptocurrency on the dark web. I know from training and experience that one of the reasons dark web vendors have multiple monikers for different vendor and customer accounts, is to prevent law enforcement from identifying which accounts belong to the same person, and who the actual person is that owns or uses the accounts.

c. The "Tor network," or simply "Tor" (an abbreviation for "The Onion Router"), is a special network of computers on the Internet, distributed around the world,

[2] Fiat currency is currency created and regulated by a government such as the U.S. Dollar, Euro, or Japanese Yen.

designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor also enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such hidden services operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software, including a browser known as "Tor Browser," designed to access the Tor network. Examples of hidden services websites are the aforementioned AlphaBay and Hansa. Tor is available on cellphones using the Android and Apple operating systems by installing an application that puts a TOR-enabled internet browser on a user's cellphone, which then routes the phone's IP address through different servers all over the world, making it extremely difficult to track.

d. Cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys (described below) used to transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object. Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a

decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.[3] Cryptocurrency is not illegal in the United States.

e. Bitcoin[4] ("BTC") is a type of cryptocurrency. Payments or transfers of value made with bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies), bitcoin ATMs, or directly from other people. Individuals can also acquire cryptocurrencies by "mining." An individual can "mine" bitcoins by using his/her computing power to solve a complicated algorithm and verify and record payments on the blockchain. Individuals are rewarded for this task by receiving newly created units of a cryptocurrency. Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it's not completely anonymous, Bitcoin allows users to

[3] Some cryptocurrencies operate on blockchains that are not public and operate in such a way to obfuscate transactions, making it difficult to trace or attribute transactions.

[4] Since Bitcoin is both a cryptocurrency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the cryptocurrency. That practice is adopted here.

transfer funds more anonymously than would be possible through traditional banking and credit systems.

f. Cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key.") A public address is represented as a case-sensitive string of letters and numbers, 26–25 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key - the cryptographic equivalent of a password or PIN - needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

g. Although cryptocurrencies such as Bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an oft-used means of payment for illegal goods and services on hidden services websites operating on the Tor network. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplaces. As of July 13, 2021, one bitcoin is worth approximately $32,000.00, though the value of bitcoin is generally much more volatile than that of fiat currencies.

h. Exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other commercially available device designed to store cryptocurrency (e.g. Trezor, Keepkey, or Nano Ledger). In addition, paper wallets contain an address and a QR code[5] with the public and private key embedded in the code. Paper wallet keys are not stored digitally. Wallets can also be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). I also know that individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

i. Bitcoin "exchangers" and "exchanges" are individuals or companies that exchange bitcoin for other currencies, including U.S. dollars. According to the Department

[5] A QR code is a matrix barcode that is a machine-readable optical label.

of Treasury, Financial Crimes Enforcement Network ("FinCEN") Guidance issued on March 18, 2013, virtual currency administrators and exchangers, including an individual exchanger operating as a business, are considered money services businesses.[6] Such exchanges and exchangers are required to register with FinCEN and have proper state licenses (if required under applicable state law). From my training and experience, I know that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, FinCEN-registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and/or the full bank account and routing numbers that the customer links to his/her exchange account. As a result, there is significant market demand for illicit cryptocurrency-for-fiat currency exchangers, who not only lack AML or KYC protocols but often advertise their ability to offer customers stealth and anonymity. These illicit exchangers often exchange fiat currency for cryptocurrencies, such as by meeting customers in person or by shipping fiat currency through the mail. Due to the illicit nature of these transactions and their customers' desire for anonymity, such exchangers are frequently able to charge a higher exchange fee, often as high as 9-10% (in contrast to registered and BSA-compliant exchangers, who may charge fees as low as 1-2%).

8. Some companies offer cryptocurrency wallet services which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses

[6] *See* "Application of FinCEN's Regulations to Person Administering, Exchanging, or Using Virtual Currencies," *available at* https://www.fincen.gov/resources/statutes-regulations/guiadance/application-fincens-regulations-persons-administering.

the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users' cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet. Alternatively, where law enforcement has obtained the recovery seed for a wallet (see above), investigators may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet

FACTS ESTABLISHING PROBABLE CAUSE
SUMMARY OF THE INVESTIGATION

9. In early December, 2019, investigators from the Central Ohio Cyber Drug Task Force (COCDTF) identified a dark web drug vendor operating under the moniker "INSTRUMENT." Information gathered from the dark web indicated that "INSTRUMENT" was active on several marketplaces advertising sales of various controlled substances that would be shipped to and from the United States. Investigators learned that in July of 2019, a drug task force in Sacramento, California, made an undercover (UC) purchase over the dark web from "INSTRUMENT" of approximately one gram of methylenedioxy-methamphetamine (MDMA).

10. Between December 2019 and May 2020, COCDTF investigators in Columbus, Ohio, made four UC purchases off the dark web marketplace "Empire" from "INSTRUMENT." The purchases included 25 dosage units of lysergic acid diethylamide (LSD) on December 12, 2019; five grams of MDMA on December 22, 2019; five dosage units of LSD on April 23, 2020; and five grams of MDMA on May 4, 2020. Each order took approximately one week to arrive in Columbus, and were sent via United States Postal Service (USPS) from different return addresses in the Minneapolis/St.Paul, Minnesota area.

11. In February of 2021, while conducting blockchain analysis on seized market place data associated with "INSTRUMENT," COCDTF investigators identified 127 transactions originating in INSTRUMENT's dark web vendor wallets that were sent to BitPay.com.

12. On February 26, 2021, COCDTF investigators sent a subpoena to Subpoenas@BitPay.com requesting all information associated with the transactions. On March 11, 2021, BitPay responded with a spreadsheet identifying 129 transactions, consisting of a total of 95.371032 bitcoin valued at approximately $43,400.11 at the time of the transactions. The spreadsheet identified the following transactions:

- Five transactions between March 9, 2014 through April 18, 2014 for approximately $6,693.96 sent to BtcTrip, a website that is no longer in existence, but a clear web search indicates it was a website designed to allow users to buy plane tickets using bitcoin.

- 105 transactions between February 24, 2014 through March 28, 2015 for approximately $24,592.62 sent to Gyft Inc., a website that allows you to buy, send, and redeem gift cards for over 200 different retailers.

- One transaction on December 07, 2014 for approximately $35.01 sent to Namecheap.com, a website that allows users to buy internet domains (website addresses).

- 17 transactions between April 29, 2014 through June 17, 2014 for approximately $12,067.56 sent to SnapCard, which allowed users to pay with bitcoin at online retailers that don't officially accept cryptocurrency. The company has since been purchased by Wyre, a payment service.

- One transaction on July 8, 2014 for approximately $10.96 sent to Warner Bros. Records. The transaction had a buyer's email address listed as Chris.Volden@gmail.com.

13. On March 15, 2021, investigators sent a subpoena to LegalPapers@Fiserv.com regarding any information on the 105 transactions conducted on Bitpay.com to Gyft, Inc. On April 6, 2021 Fiserv responded with a spreadsheet identifying 165 transactions, worth approximately $33,113.37, belonging to the same user account, identified by Gyft ID 76900276-6043-4ce8-89b0-d9211aa90090. The account listed three email addresses, Chris.Volden@gmail.com, Chris@bellslabradors.com, and Zaneisgreat@lelantos.org. All gift cards purchased were marked "self-gifted" and for big box retailers, restaurants and entertainment services. Investigators know it is common for Darknet Vendors to cash out their bitcoin in the form Gift Cards to avoid detection and report requirements from banks and law enforcement. Gyft, Inc. also listed the IP Addresses used during each transaction. A search of the IP address locations shows the transactions were conducted in, Saint Paul, Minnesota; Chicago, Illinois; Volin, South Dakota; and New York, New York; with the majority being conducted in Saint Paul, Minnesota.

14. A law enforcement database search of the email address Chris.Volden@gmail.com identified the user as Christopher Bryan VOLDEN with a date of birth of July 1, 1985. A public records check of VOLDEN listed his address as 4733 Bouleau Road, White Bear Lake, Minnesota, a suburb of Saint Paul. The prior UC drug buys from

INSTRUMENT revealed all the packages were shipped from the Minneapolis/Saint Paul, Minnesota area.

15. Investigators also learned from Homeland Security Investigations (HSI) New York that VOLDEN was being investigated in 2013 for selling bitcoin to a known dark web market vendor on the marketplace "Silk Road." At the time, HSI New York identified VOLDEN's moniker as POLYGAMUS and POLYGAMUZ. A U.S. Customs and Border Protection Database query revealed VOLDEN was the subject of three seizures, including 17.5 grams of LSD in 2016, 3.3 grams of cocaine in 2013, and 107 grams of MDMA in 2013.

16. Investigators also learned that on February 19, 2013, VOLDEN was arrested by Saint Paul Police Department (SPPD) for selling synthetic narcotics. VOLDEN admitted to SPPD that he and his girlfriend, Angela WHEELER, sold numerous controlled substance over the internet, specifically on "Silk Road" marketplace. VOLDEN explained that he had started the business and made the initial orders of their products, and WHEELER often helped him by sending/receiving orders of controlled substances through the mail. A check of VOLDEN's criminal history confirmed the SPPD arrest, but not a conviction. Investigators believe VOLDEN or WHEELER switched the dark web moniker from POLYGAMUS to INSTRUMENT after the arrest.

17. On May 6, 2021, COCDTF investigators sought and received authorization for a federal search warrant on the Google account Chris.Volden@gmail.com. On May 11, 2021, Google provided the requested information associated with that account. While analyzing the records from Google, COCDTF investigators identified various other email addresses in contact with VOLDEN, including Wheelera66@gmail.com. In VOLDEN's account, Wheelera66@gmail.com is attributed to Angela WHEELER, his known girlfriend. Also, in a

Google chat that took place on March 28, 2021, the user of Wheelera66@gmail.com identified themselves as Angela WHEELER.

18. Later in May 2021, COCDTF investigators made two additional UC purchases off the dark web marketplace "White House Market" from "INSTRUMENT." The purchases included 10 dosage units of LSD on May 11, 2021; and 50 dosage units of LSD on May 20, 2021. Following the May 11 purchase, investigators on surveillance followed VOLDEN to a United States Postal Service (USPS) drop box, and recovered an envelope with the same shipping address in Columbus that was used during the UC transaction. The envelope was photographed, repackaged, and forwarded to COCDTF investigators in Columbus. Also recovered from the same USPS drop box were thirteen (13) other envelopes matching the envelope from the UC purchase. Those envelopes were addressed to different names and addresses in multiple states including New York, Georgia, Florida, Colorado, Alabama, Oregon, Pennsylvania, Oklahoma, and other states. All of the envelopes had the same or a similar return address that the UC purchase letter had printed on it. Following the May 20 purchase, investigators on surveillance saw VOLDEN and WHEELER leave their home together in the late afternoon, but did not see them stop at a USPS drop box and were unable retrieve an envelope. COCDTF investigators, however, received the order in Columbus on May 26, 2021, that was post marked in Saint Paul, Minnesota, by USPS on May 20, 2021. USPIS investigators advised COCDTF investigators that the letter would have had to have been mailed before 6:00 PM CST on May 20 in order to be post marked on May 20. COCDTF investigators believe VOLDEN and WHEELER dropped the order in a mailbox when they were together and out of view of investigators on surveillance.

19. Law enforcement sources in Minnesota confirmed for investigators that neither VOLDEN nor WHEELER have any known employment history for the last five years. However,

in the search warrant information for VOLDEN's Google account, there were documents indicating VOLDEN paid approximately $578,000.00 in March 2021 for the home he shares with WHEELER.

20. On June 9, 2021, COCDTF investigators learned that VOLDEN and WHEELER would be traveling to Mexico with plans to leave on June 12, 2021. An update to the "INSTRUMENT" vendor profile on White House Market appeared on June 10, 2021, stating, "Gone fishing. I will return with a fully stocked menu in 3-4 weeks, maybe sooner. All orders placed with me will still get full attention. Awaiting orders will be sent on time. I do not intend on answering many messages from people without orders during my restocking period. Thanks everyone for always being awesome. The empathogen crowd is legendary." Subsequently, all of the "for sale" listings on the "INSTRUMENT" profile on White House Market were taken down.

21. VOLDEN and WHEELER returned to Minnesota on June 23, 2021. Investigators on surveillance observed them being picked up at the Minneapolis St. Paul airport and being driven home to 4733 Bouleau Road, White Bear Lake, Minnesota. The following day, the "INSTRUMENT" vendor profile on White House Market was updated again stating, "I'm slowly opening listings. Shipping will resume Saturday, June 26th. I have a handful of messages to catch up on. Please be patient. Thank you!

22. On July 14, 2021, at approximately 2:00 AM investigators made two (2) separate UC purchases from "INSTRUMENT" on the dark web marketplace "White House Market". One order was for 450 milligrams of MDMA, and the other was for five (5) dosage units of LSD. A request was made to "INSTRUMENT" to combine the orders if possible in one package to save on shipping costs. The address and name provided to "INSTRUMENT" to mail the order to was Brandon Walker, P.O. Box 92, Hilliard, Ohio 43026. On July 14, 2021, at approximately 4:29

PM investigators in Minnesota observed a 2013 blue Dodge Avenger (registration plate 415RCE) known to be utilized by VOLDEN leave his residence located at 4733 Bouleau Road, White Bear Lake, MN. Investigators were able to follow the vehicle to a United States Post Office located at 1056 Highway 96 East, Saint Paul, MN, where the vehicle drove to the area of the blue USPS collection box located in the parking lot. The blue Dodge Avenger promptly left the parking lot after driving past the collection boxes, at which time investigators identified the driver as being VOLDEN. VOLDEN drove directly back to his residence on Bouleau Road after leaving the Post Office. Investigators were assisted by USPS employees to open the collection boxes and recovered nine (9) letters similar in appearance to letters send by VOLDEN during previous UC purchases. One of the letters was addressed to Brandon Walker, P.O. Box 92, Hilliard, Ohio 43026, which was seized by the investigators. The investigators opened the letter at the DEA Minneapolis District Office, and found it to contain two separate foil like pouches. On pouch contained a small plastic zip lock baggie with brown granular substance inside which subsequently tested positive for MDMA using a field test kit, and the other pouch contained a piece of perforated paper, which subsequently tested positive for LSD.

23. Due to the evidence provided above, it is believed that Christopher VOLDEN is the head of the "INSTRUMENT' Drug Trafficking Organization (DTO).

24. This summation does not include all duties of the DTO members and is only meant to serve as a general outline. It is the belief of investigators that the duties of the DTO members change with the needs of the organization.

CONCLUSION

25. Based on the foregoing facts, I believe that there is probable cause that Christopher VOLDEN is attempting and conspiring to manufacturing, distributing or

dispensing a controlled substance, in violation of 21 U.S.C. § 841 and 21 U.S.C. §846. Accordingly, I request the issuance of a criminal complaint and arrest warrant for Christopher VOLDEN.

26. I further request that due to the ongoing nature of this investigation, the application, search warrant, and this affidavit be sealed until further ordered of the Court in order to avoid premature disclosure of the fact of this investigation and the information contained in this affidavit.

TFO

Task Force Officer Andrew Wuertz
Drug Enforcement Administration

Subscribed and sworn to before me this 20th day of July, 2021.
CONSISTENT WITH FRCrP 4.1(b)(2)(A)

~~Elizabeth A. Preston-Deavers~~ N. M. KING,
United States Magistrate Judge